Bitcoin Laundromats for Dirty Money: The Bank Secrecy Act's (BSA) Inadequacies in Regulating and Enforcing Money Laundering Laws over Virtual Currencies and the Internet

By Sheng Zhou*

Abstract:

The Bank Secrecy Act of 1970 is facing the threat of becoming unable to cope with virtual economic transactions. The rise to prominence of virtual worlds and virtual currencies in the last decade has resulted in a move by financial criminals to conduct money-laundering operations on the Internet. One such virtual currency, Bitcoin, operates as a decentralized unit of exchange with a set exchange rate to real world currencies based on supply and demand. However, existing regulations set out by the Bank Secrecy Act do not address virtual economies, leaving the burgeoning e-commerce sector in a legal grey area. Consequently, law enforcement has become increasingly aware of the threat posed by criminals who use Bitcoin and other virtual currencies to launder money outside the scope of the existing law.

This Comment explores the legal history of the Bank

* Mr. Zhou is a third-year J.D. student at American University's Washington College of Law graduating in May 2014, specializing in Corporate Law and Cyberlaw. He received his B.A. from George Washington University, in International Affairs and International Economics. Mr. Zhou can be reached at szhou89@gmail.com or through Twitter at @ShengZhouEsq.

Secrecy Act and its relevance with the growth of the virtual currency, Bitcoin. Furthermore, this Comment seeks to demonstrate the relative ease of using Bitcoin to launder money under existing regulations in comparison to traditional money laundering through a bank. In light of these loopholes, this Comment seeks to make recommendations as to ways the virtual currency legal loophole can be fixed

I. INTRODUCTION

"The [Federal Bureau of Investigation (FBI)] assesses . . . in the near term, cyber criminals will treat Bitcoin as another payment option alongside more traditional and established virtual currencies . . . and cyber criminals may increasingly use Bitcoins to purchase illegal goods and services and to fund illegal activities."[1] One of the core "illegal activities" referred to by the declassified FBI report on cybercrimes and virtual currencies is the use of virtual currencies to engage in money laundering to finance criminal activities.[2]

Money laundering is the process of taking the financial proceeds of criminal activity and making them appear legal. Generally, this process involves purposefully

---

[1] *See* FBI, BITCOIN VIRTUAL CURRENCY: UNIQUE FEATURES PRESENT DISTINCT CHALLENGES FOR DETERRING ILLICIT ACTIVITY (2012), http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf 5-6 (2012) (making the argument that law enforcement entities such as the FBI must become increasingly aware of the threat posed by Bitcoin, and highlighting the need for third party Bitcoin services to require customers to submit valid identification to complete exchange transactions in order for law enforcement measures to be effective).

[2] *Id.* at 2 ¶ 5 ("Since Bitcoin does not have a centralized authority, law enforcement faces difficulties in detecting suspicious activity, identifying users, and obtaining transaction records – problems that might attract malicious actors to Bitcoin.").

mixing illegally acquired money with legally acquired money so that it is difficult to detect and even harder for federal prosecutors to determine its origins.[3] Recent estimates of global money laundering are in the range of 1.6 trillion US dollars in a given year.[4]

In order to combat money laundering, the Group of Seven (G7) created the Financial Action Task Force (FATF), an international body dedicated to eradicating money laundering and terrorist financing to investigate solutions to new money laundering methods. The FATF has led the charge for greater regulation and accountability, offering recommendations to global governments of measures that should be implemented by both formal and informal financial sectors.[5] The organization's

---

[3] *See, e.g.*, FinCEN, Money Laundering Prevention: A Money Services Business Guide, http://www.fincen.gov/financial_institutions/msb/materials/en/prevention_guide.html (last visited Feb. 10, 2014) [hereinafter Money Laundering Prevention] (laying out the background on money laundering and its regulatory framework under the Bank Secrecy Act).

[4] *See, e.g.*, Financial Action Task Force, F.A.Q.: Money Laundering, http://www.fatf-gafi.org/pages/faq/moneylaundering/ (last visited Feb. 10, 2014) (a United Nations report estimates that in 2009, money laundering proceeds amounted to 2.7% of global GDP).

[5] *See generally* FINANCIAL ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION (2012), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf [hereinafter International Standards] (the key aspects of the FATF's recommendations are: identifying all individuals and businesses engaged in financial transactions, both formal and informal; obtaining accurate and verifiable information through which customers can be identified; and maintaining records of all financial transactions and reporting those identified as suspicious to the appropriate authorities); Financial Action Task Force, http://www.fatf-gafi.org/ (follow "About the FATF" hyperlink) (last visited Feb. 10, 2014) (lays out the functions of the FATF as an intergovernmental body created to make and enforce policies regarding international money laundering).

recommendations are adopted universally by members of the Group of 20 (G20) and are reflected in attempts by the U.S. Department of Treasury to curb money laundering in the United States.[6]

Within the United States, the Bank Secrecy Act of 1970[7] incorporates most of the FATF's recommendations. The principal goal of the BSA is to protect the access points to the United States financial system and to safeguard the American banking system from the abuses of financial crime, money laundering, and other illicit monetary activities.[8]

However, with the growing popularity of the Internet and the rise of global crime syndicates and terrorist groups in the 21st century, the framework of the BSA is no longer enough to keep up with the changing nature of global finance. A major loophole in the BSA is that the BSA's anti-money laundering provisions do not impose reporting requirements upon financial transactions not involving the physical transfer of currency.[9] Congress has

---

[6] *See, e.g.*, Money Laundering Prevention, *supra* note 3 (showing the implementation of the FATF recommendations in US Treasury requirements for prevention of money laundering).

[7] *See* Bank Secrecy Act of 1970, 12 U.S.C. §§ 1829(b), 1951-1959 (2013), *available at* http://www.law.cornell.edu/uscode/text/12/1829b; 31 U.S.C. §§ 5311-5332 (2013), *available at* http://www.law.cornell.edu/uscode/text/31/subtitle-IV/chapter-53/subchapter-II.

[8] *See, e.g.*, Jonathan P. Straub, Note, *The Prevention Of E-Money Laundering: Tracking The Elusive Audit Trail*, 25 SUFFOLK TRANSNAT'L L. REV. 515, 521 (2002) (demonstrating that the BSA requires banks to establish effective anti-money laundering programs, implement customer identification programs, and maintain transactional records for individual transactions over $10,000).

[9] *See, e.g.*, Fletcher Baldwin, *Money Laundering and Wire Transfers: When the New Regulations Take Effect Will They Help?*, 14 DICK. J. INT'L L. 413, 426 (1996) ("[Despite] seemingly comprehensive nature of the BSA's anti-money laundering provisions, none of the provisions

updated the BSA multiple times since 1970, with the most recent change being in 2001.[10] The new updates expanded existing BSA regulations by ensuring that all individuals or entities that transfer money, no matter how formal or informal, must comply with all anti-money laundering and counter-terrorist financing regulations.[11] However, the language of the updates is unclear as to the breadth of the transactions covered, which brings into question its applicability with virtual transactions.[12]

Under current frameworks, cyberspace and virtual currency exist in a legal grey area. While courts have applied property, tort, and criminal law to disputes over the Internet, those are often over disputes with calculable and foreseeable damages.[13] However, a distinguishing

---

go so far as to impose recordkeeping or reporting requirements upon financial transactions which do not involve the physical transfer of currency.").

[10] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 §§ 301-377 (2001), *available at* http://www.fincen.gov/statutes_regs/patriot/ [hereinafter PATRIOT Act].

[11] *See* Shawn Turner, Note, *U.S. Anti-Money Laundering Regulations: An Economic Approach to Cyberlaundering*, 54 CASE W. RES. L. REV. 1389, 1404 (2004) (demonstrating that the PATRIOT Act extended the definition for "financial institutions" to include foreign banks and that the BSA's broadening scope brings vast numbers of institutions within the BSA's coverage).

[12] *See* Eric J. Gouvin, *Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism*, 55 BAYLOR L. REV. 955, 982 (2003) (explaining that the PATRIOT Act does not account for "back door" techniques, and that workarounds are therefore possible for criminals and terrorists who really want to circumvent the regulations).

[13] *Accord* Susan W. Brenner, *Fantasy Crime: The Role of Criminal Law in Virtual Worlds*, 11 VAND. J. ENT. & TECH. L. 1, 1 (2008) (making the argument that crime on the Internet crosses over into the real world and vice versa, and as a result, cybercrime can and should be

difference with money laundering in cyberspace is the fact that, when done through informal channels, there is often no discernible trail. The versatility and openness of the Internet allows criminals the ability to conduct illicit financial transactions from opposite ends of the world with little to no barriers, creating a legal conundrum regarding enforcement of FATF.[14]

Consequently, this Comment seeks to examine the plausibility and possibility of legal enforcement of financial transactions using virtual currencies. In particular, it will seek to explain how Bitcoin, a popular virtual currency, operates and how it can be used to money launder over the Internet. The Comment will explore whether current money laundering statutes are and expansive enough for law enforcement authorities to enforce money laundering laws on virtual currencies. To accomplish this task, the Comment will rely on a comparison of two hypotheticals: one being a traditional money-laundering situation via a banking institution and the other being a situation involving the use of Bitcoins to move large amounts of illicit money across the Internet. Finally, this Comment seeks to make recommendations on how money laundering can be prevented with changes to current statutory regulations.

II. MONEY LAUNDERING IN CYBERSPACE: A BACKGROUND

prosecuted in the real world).

[14] *See, e.g.*, FINANCIAL ACTION TASK FORCE, MONEY LAUNDERING USING NEW PAYMENT METHODS (2010), http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf, 12-14 (outlining what some jurisdictions, such as the European Union, have done to implement FATF guidelines with regards to newer forms of payment methods).

A. The Bank Secrecy Act of 1970 and its subsequent updates established the basic framework for enforcing the prevention of money laundering within the United States.

To combat money laundering, the government recognized the importance of recording financial transactions, whereby law enforcement officials could trace the origins of large transactions within financial institutions.[15] Furthermore, under the BSA, if a banking institution suspected that a financial transaction was illicit, the bank was required to flag the transaction to the U.S. Department of Treasury.[16] Banks in the United States were obligated to file Currency Transaction Reports (CTRs) in order to qualify for federal depository insurance, but the CTRs only applied to physical transfers of currency.[17]

Since its passage, the Congress has updated the

---

[15] *See* Straub, *supra* note 8, at 522-23 (argues that one of the primary policy goals of the BSA was to create formalized procedures for financial records: "The BSA requires all formal financial institutions to file Currency Transaction Reports with the Internal Revenue Service (IRS) when conducting transactions with a single individual exceeding US$ 10,000.").

[16] *See*, *e.g.*, FINCEN, GUIDANCE ON PREPARING A COMPLETE & SUFFICIENT SUSPICIOUS ACTIVITY REPORT NARRATIVE (2003), http://www.fincen.gov/news_room/rp/files/sar_guidance_narrative.pdf [hereinafter FinCEN SAR] ("The purpose of the Suspicious Activity Report (SAR) is to report known or suspected violations of law or suspicious activity observed by financial institutions subject to the regulations of the Bank Secrecy Act (BSA) . . . information provided in SAR forms also presents the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) with a method of identifying emerging trends and patterns associated with financial crimes.").

[17] *See*, *e.g.*, Baldwin, *supra* note 9, at 426 (1996) (arguing that none of the provisions go so far as to impose recordkeeping or reporting requirements upon financial transactions which do not involve the physical transfer of currency).

BSA to keep up with the closing of money laundering loopholes. The first major update happened in 1986 with the passage of the Money Laundering Control Act[18] (MCLA), which explicitly defined the boundaries of the criminalization of money laundering.[19]

The MCLA was the subject of the Supreme Court decision in Ratzlaf v. United States,[20] a decision that brought into question the money laundering definitions established by the MCLA. The Supreme Court's opinion in the case criticized the vagueness of the language of the statute, which prompted Congress to amend the relevant statutory section and pass the Money Laundering Suppression Act (MLSA) of 1994.[21] The new act made it easier to convict an alleged criminal of money laundering without having to prove that an alleged criminal had actual knowledge that he or she was committing money

---

[18] Money Laundering Control Act, 31 U.S.C. § 5324 (2006), *available at* http://www.law.cornell.edu/uscode/text/31/5324.

[19] *See* Scott Sultzer, *Money Laundering: The Scope of the Problem and Attempts to Combat It*, 63 TENN. L. REV. 143, 166-168 (1995) (stipulating that knowingly helping launder money derived from criminal activity; knowingly engaging in transactions exceeding U.S. $10,000 that involve property from criminal activity; and knowingly structuring transactions to avoid BSA reporting were deemed to be money laundering criminal offenses).

[20] *See* Ratzlaf v. United States, 510 U.S. 135, 114 S. Ct. 655 (1994), *superseded by statute*, (deciding in a 5-4 decision, the Court held that the willfulness component of § 5324 requires the Government to prove that the defendant had knowledge that his actions were illegal and that Congress could have, but failed to, explicitly dispense with the willfulness requirement in the statute); *see also* United States v. Caro, 454 Fed.Appx. 817, 839 n.24 (11th Cir. 2012) (highlighting the statutory amendment to § 5324 in the aftermath of Ratzlaf to narrow the requirement to convict under the standard of willful knowledge, which renders the substantive decision in Ratzlaf moot).

[21] Money Laundering Suppression Act**,** Pub. L. 103–325, title IV, § 401 (Sept. 23, 1994).

laundering.[22]

The view of law enforcement towards money laundering and the BSA changed dramatically after September 11, 2001. As part of Title III of the USA PATRIOT Act,[23] Congress passed the International Money Laundering Abatement and Anti- Terrorist Financing Act (IMLAFA) of 2001 to combat the use of money laundering by terrorist organizations, namely through informal transactions. [24] For the first time, IMLAFA expanded the jurisdiction of the BSA to all financial transactions, formal and informal, and required informal money transfers to conform to the BSA financing regulations.[25] As opposed to formal financial institutions, which are mainly banks who conduct wire transfers, informal financial institutions are generally underground financial networks, collectively

---

[22] *See, cf.*, Jeremy Sanders & Jennifer Smolansky, *Financial Institutions Fraud*, 41 AM. CRIM. L. REV. 671, 719 (2004) (arguing that although the MLSA removed the willful knowledge requirement, the requirement that the alleged criminals knowingly were engaging in illegal conduct still stands).

[23] PATRIOT Act, *supra* note 10.

[24] *See id.* §§ 301-377 (2001) (recognizing the need to ensure that all appropriate elements of the financial services industry are subject to appropriate requirements to report potential money laundering transactions to proper authorities).

[25] *See* Andres Rueda, *International Money Laundering Law and Enforcement and the USA Patriot Act of 2001*, 10 MSU-DCL J. INT'L L. 141, 150-152 (2001) (laying out examples of informal financial institutions that are now covered under the BSA due to the IMLAFA, which include: money transmitters, check-cashing companies, jewelers, pawn brokers, casinos, credit-card companies, and issuers of travelers checks and money orders); *see also* Turner, *supra* note 11, at 1404 (pointing out that IMLAFA extended the definition for "money transmitter" to include any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money).

referred to as "Informal Value Transfer Systems" (IVTS).[26] These IVTS exist outside of the modern banking system and serve as an alternative to people who either do not have access to or prefer not to use the formal banking system. However, IVTS do serve a similar purpose to that of the formal systems, which is to facilitate the transfer of valued goods and money.[27]

Under the language of the IMLAFA, IVTS are referred to as "money transmitters" or "money services businesses" (MSB).[28] However, it is unclear whether

---

[26] *See, e.g.*, NIKOS PASSAS, INFORMAL VALUE TRANSFER SYSTEMS & CRIMINAL ORGANIZATIONS: A STUDY INTO SO-CALLED UNDERGROUND BANKING NETWORKS, WODC Onderzoeksnotities (1999), *available at* http://english.wodc.nl/images/on1999-4-full-text_tcm45-56889.pdf (arguing that IVTS is a system or network of people facilitating, on a full-time or part-time basis, the transfer of value domestically or internationally outside the conventional, regulated financial institutional systems); *see also* Courtney J. Linn, *One-Hour Money Laundering*, 8 U.C. DAVIS BUS. L. J. 138**,** 138 (2007) (discussing the lowered standard of scrutiny given to IVTS as compared to banks due to the wide variety of IVTS and difficulties in regulation).

[27] *See, e.g.*, FINCEN, INFORMAL VALUE TRANSFER SYSTEMS (2003), http://www.fincen.gov/news_room/rp/advisory/pdf/advis33.pdf (stating that IVTS are generally accessible around the world, even in some of the most politically unstable regions, and are reliable, efficient, and most importantly, anonymous).

[28] PATRIOT Act, *supra* note 10, § 359(b) (amending the BSA to include the clause "or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system"); see *also* FinCEN: Am I an MSB?, http://www.fincen.gov/financial_institutions/msb/amimsb.html (last visited Feb. 10, 2014) [hereinafter FinCEN MSB] (stating that MSBs are grouped into five distinct types of financial services providers: currency exchangers; check cashers; issuers, sellers, or redeemers of traveler's checks, money orders or stored value; the United States Postal Service; and money transmitters).

virtual currency transactions would fall under the definition of a MSB under the updated BSA guidelines.

B. Since the passage of the BSA, technology has updated significantly with the advent of digital currency and the global use of the Internet.

Virtual worlds arose with the proliferation of the Internet in the mid to late 1990s.[29] They exist in parallel to the real world, and users can remotely and simultaneously access them with the use of a computer and an Internet connection.[30] Because virtual worlds mirror the real world, many have virtual economies. This allows users to not only connect with one another, but also to conduct financial transactions.[31] A recent court decision involving the legal status of virtual currencies took the approach that virtual currencies are similar to that of real currencies.[32]

---

[29] *See* Beth Simone Noveck, *The State of Play*, 49 N.Y.L. SCH. L. REV. 1, 10 (2004) (making the argument that virtual worlds are becoming similar to real life and emulate societal norms in reality).

[30] *Id*. at 11 (pointing out that three-dimensional physical, interactive, and immersive spaces can be called "virtual reality" in a way that was never applicable for a simple Internet interface).

[31] *See*, *e.g.*, Posting of Brad Plummer to Wash. Post Wonkblog, http://www.washingtonpost.com/blogs/wonkblog/ (Sep. 28, 2012, 8:30 PM) (exploring the economies of several online video games and the mirroring of real-world economies in these virtual worlds where users can use virtual world currencies to purchase property within that virtual world and in the real world).

[32] *Compare* Swift v. Zynga Game Network, Inc., 2010 WL 4569889 (N.D. Cal. Nov. 3, 2010) (defining virtual currencies in the context of virtual worlds and brings into question of whether damages can be obtained from losses of virtual property) *with* Viktor Mayer-Schönberger & John Crowley, *Napster's Second Life?: The Regulatory Challenges of Virtual Worlds* 100 NW. U.L. REV. 1775**,** 1786-1790 (2006), *available at* https://www.law.northwestern.edu/lawreview/v100/n4/1775/LR100n4S

The ability to conduct real-time, in-world transactions in virtual currency that can then be exchanged for real world money has made virtual economies a thriving medium of financial transactions. The ability of users to transfer money directly from bank accounts to virtual accounts highlights the growing interconnectivity between real world financial institutions and virtual currencies.[33]

No virtual currency currently is more versatile, liquid, and convertible than a virtual currency unit known as Bitcoin. Bitcoin was created by a group of computer programmers who wanted to create a virtual currency for the Internet community as a whole.[34] The premise behind Bitcoin was to create a decentralized Internet currency where government involvement is forbidden and unnecessary.[35] To that end, Bitcoin came to fruition in 2009, based on peer-to-peer technology (P2P), meaning that Bitcoin is completely decentralized and reliant on users

---

chonberger%26Crowley.pdf (highlighting how virtual currencies in games like Second Life are convertible with real world money through third party trading sites and allow for the liquid and anonymous transfer of value between the two worlds).

[33] *See* Mayer-Schönberger & Crowley, *supra* note 32, at 1777, 1787 (pointing out that over 380,000 distinct objects changed hands in the month of July 2006 in ten million user-to-user transactions, which yielded an internal economy of US $ 10 million for that month).

[34] *See*, *e.g.*, Benjamin Wallace, *The Rise and Fall of Bitcoin*, WIRED, Nov. 23, 2011, http://www.wired.com/magazine/2011/11/mf_bitcoin/all/ (stating that the idea of digital money—convenient and untraceable, liberated from the oversight of governments and banks—had been a hot topic since the birth of the Internet).

[35] *See*, *e.g.*, Wei Dai: B-Money, http://weidai.com/bmoney.txt (last visited Feb. 10, 2014) (outlining the core philosophical principle that in a crypto-anarchy, the government is forbidden and permanently unnecessary in regards to backing Bitcoin).

for transactional management and distribution.[36] Unlike real world currencies, whose value is derived through regulation or law and backed by the state, Bitcoins have no intrinsic value due to their composition from binary numbers rather than precious metals, and their pricing is determined solely by economic supply and demand.[37]

While this may seem like a recipe for mass replications of Bitcoins, that is not the case. There is a finite amount of Bitcoins in existence at any given time, created through a process known as mining,, and the law of diminishing returns applies.[38] Mined Bitcoins are stored as computer files on a user computer, but are logged on a global public ledger. This public record is kept using a P2P network connected to the Bitcoin network, operated and

---

[36] *See, e.g.*, Wallace, *supra* note 34 (explaining the origins of Bitcoin and the initial framework of the founders to create a currency that had no central governing body).

[37] *See, e.g.*, Posting of J.P. to Babbage Blog, http://www.economist.com/blogs/babbage/ (Jun. 13, 2011, 208:30) (stating that the difference between fiat currencies and Bitcoin is that real world currencies, in principle, are answerable to its citizens, while Bitcoins comprise a community currency that is self-policing on the part of its users).

[38] *See* Andy Greenberg, *Crypto Currency*, FORBES, May 9, 2011, http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html (highlighting that Bitcoin's distributed software is set to slow production over time so that there will never be more than 21 million Bitcoins in circulation); *see also* Ogashi Tukafoto, *Bitcoin Mining for Fun and Net Loss*, SLACKTORY, Aug. 4, 2011, http://slacktory.com/2011/08/bitcoin-mining-fun-loss (stating that the rewards for Bitcoin mining get smaller and the incentive to mine switches to an incentive for collecting small transaction fees and keeping the network secure by verifying network transactions).

maintained by thousands of home computers.[39] This ledger automatically updates every time there has been a transactional exchange of Bitcoins between users. The whole process is transparent to both parties involved in the transaction and allows the parties to deal directly with one another without a third party having to authorize the transaction.[40] This ensures security as well as anonymity in transactions between users.

The mining process involves the use of special software by a Bitcoin miner that solves randomly generated complex math equations.[41] However, the problems are so complex that they usually require the resources of complete networks of computers to compute any given problem.[42] The program also caps the amount of Bitcoins that can be generated within a given period, creating a sense of

---

[39] *See, e.g.*, Barrett Sheridan, *Bitcoins: Currency of the Geeks*, BLOOMBERG BUSINESSWEEK, June 16, 2011, http://www.businessweek.com/magazine/content/11_26/b4234041554873.htm (pointing out that individual transactions are encrypted, logged by a decentralized network running on thousands of home computers, and recorded in a public ledger similar to a peer-to-peer network for file sharing).

[40] *E.g.*, J.P., *supra* note 37 (arguing that by placing the records in a P2P network, transactions are effectively secure from manipulation due to the multiple copies of the records existing on millions of computers worldwide, encrypted by public-key encryptions, ensuring the currency's security); *see also* Bitcoin Wiki: Mining, https://en.bitcoin.it/wiki/Mining (last visited Feb. 10, 2014) (stating that the ledger of past transactions is called a block chain and serves to confirm transactions to the rest of the network as having taken place, validating the legitimacy of Bitcoins in circulation).

[41] *See, e.g.*, Sheridan, *supra* note 39 (pointing out that the greater the computing power, the more Bitcoins that can be generated).

[42] *See* Greenberg, *supra* note 38 (stating that the machines in Bitcoin's mining network compute an encryption function called a "hash" on a set of random numbers, and coins are awarded when a user computes the right number chain. However very few people obtain the correct chain, thus limiting the number of coins awarded).

stability for the value of Bitcoin.[43]

Due to the prohibitively difficult nature of Bitcoin mining, most people obtain Bitcoins from Bitcoin exchange sites. Several websites provide services for the exchange of Bitcoins based on market prices of Bitcoin against real world currencies.[44] Different websites offering Bitcoin exchanges and purchases have different policies for conducting the transaction.[45] Before its closure under acrimonious circumstances in February 2014, the most popular Bitcoin exchange site was a website called MtGox. On this site, a user needed to add a state-backed currency to his or her account. Then the user could directly buy Bitcoins from MtGox using money in the linked bank account.[46] Despite the requirement of linking a bank account or Paypal account, the website facilitated exchanges in relative anonymity.[47] Other websites even

---

[43] *See, e.g.*, Jon Radoff's Internet Wonderland, http://radoff.com/blog/ (June 3, 2011) (postulating that running a mining operation on Bitcoin is similar to buying into the lottery, where computing power is exchanged for a chance to obtain Bitcoins).

[44] *See* Greenberg, *supra* note 38 (stating that about $30,000 worth of Bitcoins change hands every day in electronic transactions, spent on Web-hosting, electronics, and other commodities).

[45] *See, e.g.*, Daniel Lyons, *The Web's Secret Cash: A Novel Version of Money is Sprouting Online, Letting People Shop In Complete Anonymity*, NEWSWEEK, June 19, 2011, http://www.thedailybeast.com/newsweek/2011/06/19/the-web-s-secret-cash.html (illustrating the free market nature of the Bitcoin trading price, which fluctuates based on demand and can range widely in value).

[46] *See generally* MtGox, https://www.mtgox.com/ (last visited Feb. 10, 2014) (outlining the function of the service and requirements that are needed to have an account on MtGox and to engage in financial transactions using the website).

[47] *E.g.*, Bitcoin Wiki: MtGox, https://en.bitcoin.it/wiki/MtGox (last visited Feb. 10, 2014) (stating that MtGox operates as a facilitator of exchange of Bitcoins between users and not as an overseer or regulatory agent).

offer to facilitate transfers of Bitcoins in person, organizing face-to-face meetups for people interested in doing so.[48] Today, many websites, and even real world stores, accept Bitcoins as legal currency in exchange for goods and services.[49]

> C. While the typical fact patterns for money laundering through traditional methods and through using Bitcoins are similar, there are major differences in the ability of law enforcement to track down the culprits.

In the first scenario, a crime syndicate, in order to launder their illegally obtained money, makes six deposits with a multinational Bank A, with branches in the US. One deposit is $12,000, while the other five were below $10,000, totaling $35,000 worth of deposits. The deposit of $12,000 was not split into smaller denominations. While the bank allowed the deposits to be made, the deposit of $12,000 triggered the requirement for the bank to file a

---

[48] *See, e.g.*, Trade Bitcoin: Local Trading, http://tradebitcoin.com/about/ (last visited Feb. 10, 2014) (portraying the service provided by the website as a facilitator of face-to-face meetings of Bitcoin exchanges for people in a user's area).

[49] *See* Psuedonymous, *I Spent a Coin (and I Liked It) — How I Bought Lunch With Bitcoins*, NYMAG, June 28, 2011, http://nymag.com/daily/intelligencer/2011/06/i_spent_a_coin_and_i_liked_it.html (detailing how the author bought lunch at a local New York City restaurant using Bitcoins and illustrates the growing acceptance of Bitcoins as another form of currency); *see also The Tuesday Podcast: Bitcoin* (NPR Planet Money podcast Jun. 12, 2011), http://www.npr.org/blogs/money/2011/07/13/137795648/ (explaining the increasing use of Bitcoins within the US to purchase goods and services online and in the real world).

CTR to the IRS.[50] The bank did not fill out a Suspicious Activity Report with the CTR and the deposits were processed.[51]

A week after the criminal syndicate made the deposits, they transferred the deposits into two offshore Cayman Island banks, and then back to another American bank, Bank B. The withdrawal of the $12,000 prompted another CTR to be filed by Bank A and the deposit of $12,000 a week later to Bank B prompted Bank B to file another CTR.[52] At this stage, three CTRs have already been submitted to the IRS by two American banks. The close proximity of these transactions alerted the government and the FBI began to investigate the transactions.[53] The FBI determined that the $12,000 dollars had routed between several offshore accounts between Bank A and Bank B. The pattern of the money

---

[50] *See* FINCEN, THE FINCEN CURRENCY TRANSACTION REPORT & DESIGNATION OF EXEMPT PERSONS REPORT, http://www.fincen.gov/whatsnew/pdf/CTR&DOEPRecordedVersion-PDFslides.pdf (last visited Feb. 10, 2014) (laying out the purpose of the CTR to report currency transactions in excess of $10,000 and gives technical information on the proper methodology to fill out a CTR).

[51] *See, e.g.*, FinCEN SAR, *supra* note 16, at 1 (stating that Suspicious Activity Reports are only required to be filled and submitted along with a CTR if the financial institution has reason to believe that the transaction involved suspicious funds).

[52] *See* Sultzer, *supra* note 19, at 148-151 (outlining the steps of a traditional money laundering operation, involving rerouting the funds through other banks as a common method to escape detection from law enforcement and to make the money seem legitimately derived from different sources).

[53] *See, e.g.*, Baldwin, *supra* note 9, at 441 (1996) (postulating that FinCEN uses artificial intelligence to aid in the identification of money launderers by analyzing a compilation of data, including CTR's, to identify and monitor potentially illegal patterns of behavior characteristic of money laundering).

points towards a potential money-laundering situation.[54]

A week after investigations started, the FBI noticed that money from six accounts at Bank B, which had arrived around the same time, one of which was the $12,000 account, began to be withdrawn. Agents obtained a warrant and detained the men who were making the transactional withdrawals from Bank B. The agents were able to ascertain to a reasonable extent that the laundered money came from an illegal meth operation. On top of all the other criminal charges, the FBI wants to charge the defendants under the Bank Secrecy Act for money laundering.[55]

In the second scenario, another criminal syndicate has made the decision to turn to a far more lucrative and accessible way to money launder, by using virtual currency. They decided that Bitcoin was the best way to quickly and anonymous launder tens of thousands of dollars of cash from their illegal operations. A syndicate member created several accounts on MtGox and linked these accounts to his Dwolla account.[56] Fifty thousand dollars' worth of illegally acquired funds were put in his Dwolla account and used as the basis for his transactions on MtGox. Assuming that the exchange rate of Bitcoins to US Dollars was 1 BTC

---

[54] *See* Rueda, *supra* note 25, at 164 (detailing the assistance of FinCEN guidelines in helping law enforcement officers and prosecutors initiate and facilitate investigations into money laundering).

[55] *See* 18 U.S.C. § 1957 (2006), *available at* http://www.law.cornell.edu/uscode/text/18/1957 (stating that prosecutors have to know that they can prove the members involved in the laundering operation knowingly engaged or attempted to engage in a monetary transaction in criminally derived property of a value greater than $10,000).

[56] *See*, *e.g.*, Dwolla, https://www.dwolla.com/about (last visited Feb. 10, 2014) (explaining that Dwolla is a cash based payment network that can be used to buy goods and services online, similar to Paypal, but without the need to link the account to a formal financial institution).

for $20,[57] he was able to successfully purchase 2,500 Bitcoins from other users around MtGox. After purchasing these Bitcoins, he proceeded to use the same website to sell off his 2,500 Bitcoins.[58] Over the course of the month, the he was able to sell all his coins, at a minor profit, due to unusually higher demand for the coins. He then withdrew about $52,000 from his Dwolla account.[59]

Posing as a Bitcoin buyer, federal agents had been watching MtGox for unusually large transfers of Bitcoins. The purchase of 2,500 Bitcoins across several accounts and the instant resale of these Bitcoins raised suspicions among federal investigators. However, due to the highly anonymous nature of transactions with Bitcoin, the investigation could not produce the names and locations of the buyers and sellers.[60] Since data regarding each client is stored locally and not in a central server, attempts to subpoena MtGox would not produce anything to help federal investigators.[61] However, during the transaction with one of the launderer's accounts, FBI agents were

---

[57] *Accord* Coinmill.com: The Currency Converter, http://coinmill.com/BTC_USD.html (last visited Mar. 1, 2014) (showing the current exchange rate between USD and BTC to be around $613.90 to 1 BTC).

[58] *See* Bitcoin Wiki: MtGox, *supra* note 47 (giving instructions on how users can buy and sell on MtGox using Dwolla as a cash basis for all their transactions).

[59] *See*, *e.g.*, Dwolla, *supra* note 56 (advertising the fluidity and ease of moving cash around with the Dwolla service).

[60] *See*, *e.g.*, Greenberg, *supra* note 38 (illustrating that there is no centralized storage of funds, so accounts cannot be frozen by authorities such as law enforcement or PayPal administrators).

[61] *See*, *e.g.*, Sheridan, *supra* note 39 (stating that individual transactions are encrypted, logged by a decentralized network running on thousands of home computers, and recorded in a public ledger).

successful in obtaining his IP Address,[62] which indicated that the seller was based in the United States.

III. RECENT UPDATES TO THE BSA DO NOT ENCOMPASS TRANSACTIONS INVOLVING DIGITAL CURRENCY, CREATING SCENARIOS WHERE ILLEGAL ACTIVITIES CAN OCCUR WITHOUT REGULATION.

Despite the recent attempts by FinCEN to encompass internet transactions under the umbrella of MSBs, Congress has not updated the statutory framework since 2001. At present, the broad academic nature of the definition of IVTS and MSB does not allow for a clear legal delineation of whether virtual currency transactions fall under the definitions of the BSA.[63] Furthermore, the pseudonymous nature of Bitcoin means that investigators have very limited means to track Bitcoin transactions. Even if the FBI was aware of major money-laundering operations happening through the usage of Bitcoin exchange sites, there is very little that they can do to track

---

[62] How Stuff Works: What is an IP Address?, http://computer.howstuffworks.com/internet/basics/question549.htm (last visited Feb. 10, 2014) (explaining that an Internet Protocol address (IP) is registered to an individual computer as it is connected to the Internet in a given session, similar to a home address).

[63] *See* Posting of Dennis Lormel on Counterterrorism Blog, http://counterterrorismblog.org/2008/05/two_easily_exploitable_vulnera.php (May 21, 2008, 15:41 EST) (reaffirming that MSBs refer to five distinct types of financial services providers and nothing more).

down the source of transactions.[64] This is highlighted by the recent closure of MtGox and the purportedly missing $450 million worth of Bitcoins, demonstrating the limited ability of the authorities, and even the site administrators, to track and locate Bitcoins when they seemingly vanish into the Internet.[65]

The current framework is inadequate in preventing cyber laundering because it does not directly acknowledge the existence of virtual currencies and a clear definition.[66] In analyzing the factual hypotheticals posited in the last section, it becomes clear that the existing legal framework is appropriate for traditional money laundering, but is inadequate in addressing money laundering using virtual

---

[64] *See* Thomas Lowenthal, *Bitcoin: inside the encrypted, peer-to-peer digital currency*, ARS TECHNICA (Jun. 8, 2011) http://arstechnica.com/tech-policy/2011/06/bitcoin-inside-the-encrypted-peer-to-peer-currency/ (pointing out that Bitcoins can be as anonymous as the user wants); *but see* Jon Matonis, *Bitcoin's Greatness Not Realized By Succumbing To Regulation*, FORBES (Dec. 9, 2012) http://www.forbes.com/sites/jonmatonis/2012/12/09/bitcoins-greatness-not-realized-by-succumbing-to-regulation/ (arguing that Bitcoin users prefer the anonymity of Bitcoin and that the self-regulating nature of Bitcoin does not require the government to step in and regulate the transactions); *but see* Sarah Meiklejohn, et. al., *A Fistful of Bitcoins*, 38 ;LOGIN: 6 (December 2013) http://cseweb.ucsd.edu/~smeiklejohn/files/login13.pdf (demonstrating the potential deanonymization techniques that law enforcement could use to locate stolen Bitcoins).

[65] *See* Rachel Abrams, Matthew Goldstein, and Hiroko Tabuchi, *Erosion of Faith Was Death Knell for Mt. Gox*, NEW YORK TIMES (Feb. 28, 2014) http://dealbook.nytimes.com/2014/02/28/mt-gox-files-for-bankruptcy/?partner=rss&emc=rss&smid=tw-nytimes (pointing out that MtGox lost hundreds of thousands of Bitcoins and cannot locate where these Bitcoins have gone).

[66] *See, e.g.*, Straub, *supra* note 8, at 527 (2002) (pointing out that existing regulations create a system to report transactions that occur in financial transactions, but the very nature of e-money is that there is little to no reporting requirement).

currencies. However, in order to bring virtual currencies into the realm of governmental regulation, it will be necessary to confront privacy issues and fundamental changes in the way the government treats the Internet.[67]

> A. U.S. law enforcement's awareness of the potential threat of the use of virtual currencies, such as Bitcoin, to launder money outside the scope of existing law illustrates a current inadequacy in regulation.

At its core, Bitcoin fits within the parameters of an IVTS, and with its decentralized nature and its mobility, it creates the ability to move large amounts of money at once without triggering BSA safeguards.[68] While it does not explicitly fall within any category of the IMLAFA definition of a MSB, it is clear that Bitcoin is an informal

---

[67] *Compare* Michael W. Loudenslager, *Allowing Another Policeman on the Information Superhighway: State Interests and Federalism on the Internet in the Face of the Dormant Commerce Clause*, 17 BYU J. PUB. L. 191, 256 (2003) (arguing that both state and federal courts can uphold legislation that attempts to regulate commerce on the Internet, from a case-to-case basis) *with* Lawrence B. Solum, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815, 947 (2004) (advocating for the use of careful regulation of the Internet, to be perceived through multiple layers of activity where regulations would only target specific layers and not the Internet as a whole).

[68] *See, e.g.*, Mike Masnick, *Senator Schumer Says Bitcoin Is Money Laundering*, TECHDIRT (Jun. 6, 2011), http://www.techdirt.com/articles/20110605/22322814558/senator-schumer-says-bitcoin-is-money-laundering.shtml (highlighting fears from Congress over Bitcoin laundering).

financial institution.[69] Consequently, under the murky definition of MSBs as established by the IMLAFA, how would Bitcoin fare under attempts by law enforcement to enforce BSA standards on Bitcoin transactions? If the government does manage to hold someone accountable for money laundering using Bitcoins, they must prove the presence of three elements, as outlined by the BSA.[70]

Attempts by the US Department of Treasury to strengthen the definitions of MSB to include greater variations of IVTS,[71] along with an FBI report highlighting the threat posed by cyber criminals, seem to illustrate the reality of the threat of money laundering using virtual currencies and the inability of current regulations to address the concerns of virtual money laundering.[72]

B. The current BSA rules would be able to regulate and enforce anti-money laundering laws in a case of

---

[69] *See, e.g.*, Bitcoin Money: FinCEN Brings KYC Requirements to Bitcoin?, http://www.bitcoinmoney.com/post/8412471372/fincen-prepaid-access-final-rule (last visited Feb. 10, 2014) [hereinafter FinCEN KYC] (including the possibility that even businesses outside the U.S. conducting money transfer over the Internet could still be classified as U.S. MSBs and that the definition no longer requires that a MSB be a business, but can be any individual who receives funds in exchange for a stored value might be considered an MSB).

[70] *See* U.S. v. Carucci, 364 F.3d 339, 343 (1st Cir. 2004), *available at* https://www.casetext.com/case/us-v-carucci/ ("(1) the defendant engaged or attempted to engage in a monetary transaction with a value of more than $ 10,000; (2) the defendant knew that the property involved in the transaction had been derived from some form of criminal activity; and (3) the property involved in the transaction was actually derived from specified unlawful activity.").

[71] *See, e.g.*, FinCEN KYC, *supra* note 69 (pointing towards the new ruling from FinCEN that attempts to expand the definition of MSB to encompass more IVTS).

[72] *See generally* FBI, *supra* note 1 (outlining that the FBI views cyber criminals who use virtual currencies to money launder using the Internet as a potential threat).

> money laundering using formal financial institutions.

Under traditional money laundering, there are usually three steps: placement, layering, and integration.[73] Placement involves changing the money from criminal activities into a less suspicious form, most commonly with a deposit at the bank.[74] Layering involves the wire transfer of funds from numerous accounts to other accounts in an attempt to hide the funds' true origins.[75] Integration, the final step, involves movement of the layered funds, their origins no longer traceable, into the global financial world, where the launderers dilute the dirty money with legitimate money.[76]

The federal government has jurisdiction to press charges against the defendant as long as the government

---

[73] *See, e.g.*, Money Laundering Prevention, supra note 3 (stating that the focus of FinCEN's strategy is to stop money launderers at the placement stage, before the layering process can disguise the funds' origin).

[74] *See* Sultzer, *supra* note 19, at 148 (illustrating that the placement stage of money laundering is the hardest stage for money launderers to commit and that launderers will often route cash through a front operation in order to give the funds a legitimate cover when they are deposited into a financial institution).

[75] *Id.* at 150 (highlighting the fact that layering is the process where the origins of the funds being laundered are masked through dispersions to other banks, usually outside the United States).

[76] *Id.* at 151 (stating that funds are integrated into the legitimate financial world through forms such as letters of credit, bonds, and other securities, prime bank notes and guarantees); *accord* Greg Dekermenjian, *Developments In Banking And Financial Law: 2005: Xiv. Anti-Money Laundering*, 25 ANN. REV. BANKING & FIN. L. 137, 141-143 (2006) (arguing that traditional money laundering laws has extensive programs to prevent acts of money laundering happening in formal financial institutions).

has enough evidence to press for a case.[77] The bigger question is whether the government will have fulfilled the three elements, as stipulated by the BSA, to convict the defendants of money laundering. In order to find the defendants guilty, the government must prove the existence of all three elements: (1) the defendant engaged or attempted to engage in a monetary transaction with a value of more than $ 10,000; (2) the defendant knew that the property involved in the transaction had been derived from some form of criminal activity; and (3) the property involved in the transaction was actually derived from specified unlawful activity.[78]

Element one is fulfilled with the deposit and withdrawal of the $12,000 in Bank A, as certified by Bank A's CTRs. Bank B's CTR can also corroborate the fact that a defendant engaged in a financial transaction above $10,000. Assuming the FBI investigation has some form of evidence linking the defendant to the crime syndicate and that the FBI reasonably believed that the $12,000 came from the drug operation, the crime will also fulfill the second element of the statute. It would seem unlikely for the FBI to pursue a case if there was insufficient evidence

---

[77] *See* 18 U.S.C. § 1956(e) (2006), *available at* http://www.law.cornell.edu/uscode/text/18/1956 (laying out the jurisdictional basis for different branches of the US government, including the Department of Homeland Security and the Department of Justice to investigate violations of § 1956 prohibiting the laundering of monetary instruments).

[78] *See*, *e.g.*, 18 U.S.C. § 1957, *supra* note 55 (ruling that the statute not only lays out the general elements, but also defines a 'monetary transaction' as "deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds or a monetary instrument' in § f); *see also* U.S. v. Carucci, *supra* note 70, at 343 (reaffirming the First Circuit's interpretation of the language of 18 U.S.C. § 1957 with regards to the elements that the government has to prove in order to invoke a conviction for money laundering).

as to this regard. Element three is closely linked with element two and, assuming the FBI has evidence or testimony linking the money to the meth operation, then this element is fulfilled.

With all three elements fulfilled, the Department of Justice will most likely win in a court against the defendant.[79] The government could charge the other defendants who were not directly engaged in the $12,000 transaction with at least conspiracy to commit money laundering, but the case against the primary defendant of money laundering in violation of the BSA is straightforward.[80] This result is not surprising as the legislative intent of the BSA was to stop this form of money laundering through formal financial institutions.[81]

> C. Money laundering using Bitcoin is a definite possibility, as the nature of Bitcoin allows money launderers to remain anonymous and difficult for law enforcement to detect, and current legislation appears to be inadequate in linking virtual money launderers to the crime.

Assuming that federal prosecutors are held to the

---

[79] *Id.* (pointing out that the fulfillment of all three elements of money laundering in the statute constitutes a violation of the BSA and a money laundering crime).

[80] *See* 18 U.S.C. § 371 (2006) *available at* http://www.law.cornell.edu/uscode/text/18/371 ("If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.").

[81] *See*, *e.g.*, Rueda, *supra* note 25, at 201 (arguing that the PATRIOT Act strengthens the U.S. financial transaction reporting system to levels never seen before and that the language is very broad in scope).

same standard as they are for formal financial transactions, they must look at the three elements required by the BSA to prosecute the syndicate member for money laundering.[82] Despite the expansion of the BSA under IMLAFA to informal transfers, virtual currencies exist in a legal grey area concerning classification.[83] Under the definition of MSBs that was set out in IMLAFA, the category that a Bitcoin service like MtGox would fall under would most likely be considered to be either a currency exchanger or money transmitter.[84]

However, this classification in itself is not completely accurate of the service that MtGox provides for its users. Prosecutors could attempt to explain that MtGox would fall under either of those categories, but they would have to prove that the primary purpose of MtGox is to exchange currencies and/or to transfer money between people.[85] This classification is tenuous at best, as MtGox only facilitates the exchange of Bitcoins, units that are not statutorily real currency and are unregulated by the

---

[82] *See*, *e.g.*, U.S. v. Carucci, *supra* note 70, at 343 (reiterating the three requirements created by Congress with the passage of IMLAFA in order for a defendant to be convicted for money laundering).

[83] *See*, *e.g.*, FinCEN KYC, *supra* note 69 (stating that FinCEN is attempting to expand MSBs to encompass virtual currencies, current statutory law remains outdated to address virtual currencies).

[84] *See*, *e.g.*, FinCEN MSB, supra note 28 (laying out the current legal parameters of what is defined to be a MSB, and thus under the regulatory framework of the BSA to be narrow in scope and not all encompassing).

[85] *See*, *e.g.*, Bitcoin Wiki: MtGox, *supra* note 47 (explaining that MtGox operates as a facilitator of exchange of Bitcoins between users, does not have an overseeing role in transactions, and does not require detailed personal information from users).

government.[86] Furthermore, even if prosecutors were successful in classifying the transactions to be within the purview of the BSA, they would have a difficult time in proving all three elements required to convict for money laundering under the BSA.[87] The only element that could be proven with certainty is that transactions over $10,000 were made, but due to the anonymous nature of the Bitcoins exchange process, it would be near impossible to prove that the money was from illegal sources without help from a third party source, like an informant.[88]

Most likely, without the legal backing of formally declaring virtual currencies to be an IVTS, it is highly unlikely that prosecutors can make the argument that MtGox is a MSB.[89] Consequently, because of this tenuous connection between MtGox and its classification as a MSB, it would seem likely that MtGox would not fall within the

---

[86] *See* Posting of C.F. to Babbage Blog, http://www.economist.com/blogs/babbage/2011/10/virtual-currencies (Oct. 21, 2011, 12:47) (stating that when Bitcoin emerged in 2009, the Internet community immediately embraced the idea of an unregulated currency free from meddling governments).

[87] *See* 18 U.S.C. § 1957, note 55 ((1) the defendant engaged or attempted to engage in a monetary transaction with a value of more than $ 10,000; (2) the defendant knew that the property involved in the transaction had been derived from some form of criminal activity; and (3) the property involved in the transaction was actually derived from specified unlawful activity).

[88] *See* Lowenthal, *supra* note 64 (pointing out that Bitcoin transactions can be as anonymous as the user wants and the process does not require the registration of a real name and address).

[89] *See, e.g.*, FinCEN MSB, *supra* note 28 (illustrating the conundrum that it would be very difficult to classify what service MtGox would be considered to facilitate, especially with the tricky legal status of Bitcoin as a whole).

reach of the BSA and its regulations.[90] While the deposit of proceeds made from Bitcoin laundering through traditional bank accounts may potentially allow investigators to locate the identities of the virtual money launderers, the patterns attributed to traditional money laundering are not present.[91] Bitcoin-laundered money would appear to be legitimate when deposited into bank accounts, as funds would not be arriving from other banking institutions, but from an online source.[92] Banks will still file CTRs regarding their deposits, but the necessary paper trail to spot money laundering does not exist prior to the transfer of money from a virtual account to a bank.[93] Consequently, deposits made from the proceeds of the Bitcoin exchanges into conventional banking institutions would trigger a CTR, but would be unlikely to raise suspicion due to the direct nature of the

---

[90] *Compare id.* (stating that MSBs are grouped into five distinct types of financial service providers: currency exchangers; check cashers; issuers, sellers, or redeemers of traveler's checks, money orders or stored value; the United States Postal Service; and money transmitters) *with* Bitcoin Wiki: MtGox, *supra* note 47 (explaining that MtGox operates as a facilitator of exchange of Bitcoins between users, which does not seem to fit into the definition of an MSB as laid out by FinCEN).

[91] *See*, *e.g.*, Money Laundering Prevention, *supra* note 3 (highlighting that the current strategy towards catching money launderers is to stop money laundering at the first stage, before origins of funding can be masked).

[92] *See*, *e.g.*, Dwolla, *supra* note 56 (explaining that Dwolla exists as a virtual bank account from which money can be drawn to conduct Bitcoin transactions).

[93] *See*, *e.g.*, Sultzer, *supra* note 19, at 150 (highlighting the fact that layering is the process whereby the origins of the funds being laundered are masked, but the funds retain a paper trail of transactions between banks).

transactions from virtual account to bank account.[94]

Furthermore, investigators would be unable to bind websites like MtGox to BSA limitations due to the legal grey area in which MtGox operates, with its unclear MSB status.[95] Consequently, the money launderers would most likely escape without facing formal charges.[96] The patterns presented demonstrate that the use of Bitcoins to launder money attacks is more than merely a theoretical academic discussion.

D. Traditional money laundering schemes and Bitcoin laundering schemes are similar in their intents, but are clearly different in their implementations and regulations.

At its core, money laundering with Bitcoins is similar to that of laundering through formal banking institutions. Both are means to the same end: to dilute the legality of illegally acquired money.[97] Their divergence in regulation is a purely legal one. Governments regulate

---

[94] *See*, *e.g.*, Greenberg, *supra* note 38 (illustrating that no paper trail exists for transactions that occur using virtual accounts such as Paypal beyond the immediate transaction in or out of the account).

[95] *See* Lormel, *supra* note 63 (reaffirming that MSBs refer to five distinct types of financial service providers and nothing more).

[96] *Accord* Daniela Rosette, *The Application Of Real World Rules To Banks In Online Games And Virtual Worlds*, 16 U. MIAMI BUS. L. REV. 279, 302 (2008) (arguing that in order for any form of regulation to be effective, it requires the tracking of money flows and logging of transactional activity, requirements Bitcoin does not meet).

[97] *See*, *e.g.*, Stephen I. Landman, Note, *Funding Bin Laden's Avatar: A Proposal for The Regulation Of Virtual Hawalas*, 35 WM. MITCHELL L. REV. 5159, 5162 (2009) (making the argument that terrorists using virtual worlds and virtual currencies to money launder to finance their operations are able to do so under the current framework); *see also* Rueda, *supra* note 25, at 141 (the goal of traditional money laundering is to make illegal funds seem legitimate).

formal banking institutions far more due to decades of experience dealing with financial crimes that occur through those channels.[98] All statutory updates passed by Congress since the passage of the BSA were primarily to deal with traditional formal money laundering through formal financial institutions. However, with the advent of the Internet within the last twenty years, the law has yet to keep up with developments on the Internet.[99] The classifications of MSBs under the IMLAFA update to the BSA were made with traditional informal financial transfers in mind, not with the idea of combatting cybercrimes.[100] Consequently, this discrepancy between the reality of vibrant Internet transactions and the legal definition of IVTS creates a legal blind spot, which legally-aware criminals can easily exploit.[101]

---

[98] *See* Duncan E. Alford, *Anti-Money Laundering Regulations: A Burden on Financial Institutions*, 19 N.C.J. INT'L L. & COM. REG. 437, 466-467 (1994) (postulating that due to strict regulations and experiences with money laundering in formal financial institutions, launderers are using informal institutions to conduct money laundering).

[99] *See* Landman, *supra* note 97 (arguing the inadequacy of the current state of the law regarding virtual money laundering and pointing out that existing BSA regulations allow for loopholes that can be exploited by terrorists and criminal organizations).

[100] *See, e.g.*, 31 U.S.C. § 5312(a)(2), *available at* http://www.law.cornell.edu/uscode/text/31/5312 (defining the scope of 'financial institutions' under BSA); *see also* Straub, *supra* note 8, at 533 (arguing that in order to curb new techniques in money laundering while simultaneously promoting technological development, the government should focus on regulating the transaction).

[101] *See* Brian Monroe, *ATM Cards Tied to Virtual Worlds a "Money Launderer's Dream,"* MONEY LAUNDERING ALERT, Dec. 2007, *available at* https://www.world-check.com/media/d/content_pressarticle_reference/Rijock_Fortent_20071120.pdf (showing an example of a potential money laundering operation that can happen over the Internet due to the lax regulations at the present time).

Consequently, as demonstrated by the two hypotheticals posited in this Comment, similar scenarios using different methods result in vastly different outcomes. There is far more room to maneuver for criminals when conducting money laundering operations over the Internet using virtual currencies.[102] The very nature of the Internet makes it difficult for law enforcement to crack down on illegal activities, but that does not have to be the case.[103]

Bitcoins epitomize the unregulated nature of Internet activities. Recent demand for Bitcoins by users around the world resulted in a dramatic increase in the price of Bitcoins, which was trading at an all-time high above $1,200 in November 2013.[104] The ability of a Bitcoin user to use Bitcoins to accomplish a wide spectrum of tasks on the Internet, both legal and illegal, is a cause for concern.[105] Additionally, the potential of the law to regulate the use of Bitcoins is limited due to the global and anonymous nature of the Internet. Consequently, it is more likely for legislators to extend the existing legal framework to cover such transactions, rather than create new legal

---

[102] *See*, *e.g.*, Straub, *supra* note 8, at 529 (advocating that statutory reforms and changes to the current regulatory scheme need to be made to account for the growth of virtual currencies in order for money laundering laws to remain effective).

[103] *See* Solum, *supra* note 67, at 947 (advocating for the use of careful and targeted layer-approach to regulation of the Internet, where specific regulations only affect certain Internet activities and not others).

[104] *E.g.*, Maureen Farrell, *Bitcoin Now Tops $1,200*, WALL STREET JOURNAL, Nov. 29, 2013, http://blogs.wsj.com/moneybeat/2013/11/29/bitcoin-now-tops-1200/ (discussing the skyrocketing value of Bitcoin and fears of a bubble).

[105] *But see* Timothy B. Lee, *Porn, gambling, and malware: Bitcoin as the 'Net's Wild West*, ARSTECHNICA, Jun. 8, 2012, http://arstechnica.com/business/2012/06/porn-gambling-and-malware-bitcoin-as-the-nets-wild-west/ (arguing that despite the laissez-faire nature of Bitcoins, federal regulators should not attempt to regulate it as it would stifle potential innovation).

mechanisms.[106] Even then, the ability of the government to regulate any aspect of Internet activity requires a fundamental rethink of the Internet's base structure as an open-source platform.[107]

> E. The regulation of Bitcoin will result in the unavoidable sacrifice of privacy for financial transactions on the Internet and a push for a change in the way the Internet is viewed as an open-source network.

Bridging the gap between real world money laundering and virtual money laundering from a regulatory perspective requires a major leap concerning the structure of the Internet.[108] The major problem that law enforcement

---

[106] *But cf.* Bitcoin & Trading Titan Blog, *What U.S. Regulations Apply to Bitcoins as Commodities?* http://blog.bitcointitan.com/post/17789738826/what-u-s-regulations-apply-to-bitcoins-as-commodities (last visited Feb. 10, 2014) (showing a working understanding of Bitcoins as a commodity under US securities law, which does not involve the creation of brand new legislation, but a mere extension of existing statutory frameworks).

[107] *See, e.g.*, Jay P. Kesan and Andres A. Gallo, *Optimizing Regulation of Electronic Commerce*, 72 U. Cin. L. Rev. 1497, 1622 (2004) (concluding that in its current state, the Internet is too widespread and accessible globally for successful regulation to occur and that lack of clear enforcement hurts e-commerce).

[108] *See* Thomas B. Nachbar, *Paradox and Structure: Relying on Government Regulation to Preserve the Internet's Unregulated Character*, 85 MINN. L. REV. 215, 316-17 (2000) (arguing that proposed government regulations to extend governmental oversight over the Internet would limit the freedom of Internet users and would destroy the Internet's value as a source for free exchange). *But see* Michael A. Geist, *The Reality of Bytes: Regulating Economic Activity in the Age of the Internet*, 73 WASH. L. REV. 521, 570 (1999) (postulating that Internet regulation is necessary to ensure unhindered economic activity on the Internet and that regulation should come from every aspect of government).

encounters with services such as MtGox is the anonymous nature of its user base.[109] Without being required to verify their real identities and addresses, users can maintain a trading account on MtGox, where their activities are unregulated by the website.[110]

Regulation of sites like MtGox would inevitably require that such sites maintain a record of their users' personal information and a system of identification verification.[111] However, such requirements would require the cooperation of multiple states and would create issues of privacy and information security.[112] Consequently, in order for current anti-money laundering laws to be effective on the Internet, a degree of privacy will invariably have to be sacrificed.

IV. RECTIFYING THE LEGAL PURGATORY OF VIRTUAL CURRENCIES WITHIN THE BANK SECRECY ACT

Congress must take additional measures to curb the use of virtual currencies to launder money and bring regulation of those virtual currencies under the umbrella of

---

[109] *See, e.g.*, Bitcoin Wiki: MtGox, *supra* note 47 (stating that the underlying philosophy behind Bitcoin exchange revolves around anonymity).

[110] *Id.* (stating that MtGox does not require personal information for a user to have an account on the website and to engage in trades).

[111] *See* Solum, *supra* note 67, at 922 (arguing that digital identification verification is an easy solution for regulation of the Internet, which can be achieved securely, privately, and anonymously, with minimal breaches of privacy).

[112] *Compare* Steven A. Hetcher, *The Emergence of Website Privacy Norms*, 7 MICH. TELECOMM. TECH. L. REV. 97, 145-46 (2001) (advocating for increased self-regulation of websites to ensure high standards for privacy on the Internet) *with* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1701 (1999) (arguing that the proliferation of private information on the Internet of its users has a negative effect on society).

the BSA. Creating a level of parity between formal financial institutions and IVTS would foster similar levels of responsibility and awareness for illegal activities involving financial crimes.[113] It would effectively close the loophole that currently exists for money launderers to use virtual currencies in laundering illegally acquired funds. To accomplish this, Congress must pass new updates to the BSA to address the new issues surrounding the advent of the Internet.[114]

> A. The Bank Secrecy Act must be updated to classify Internet transactions as IVTS and virtual currencies as MSB in order to expand the purview of the BSA.

Under the existing definition of IVTS, virtual worlds on the Internet exist in a grey area where legal boundaries are nebulous.[115] In order to rectify this problem, the government should update regulations to reflect the need for every IVTS to register with the Treasury Department.[116] Once websites dealing with financial transactions of virtual currencies are officially

---

[113] *See* Landman, *supra* note 97, at 5181 (postulating that once existing BSA regulations are expanded to cover virtual worlds, law enforcement and intelligence officials can begin cracking down on one of the last remaining unregulated methods for transferring terrorist funds).

[114] *See* Rosette, *supra* note 96, at 301 (arguing that after the passage of the PATRIOT Act in the US, the FATF released a number of recommendations attempting to expand existing MSB regulations into more informal systems).

[115] *See*, *e.g.*, Money Laundering Prevention, *supra* note 3 (stating that FinCEN does not address virtual currencies or virtual transactions in their guidelines).

[116] *See* 31 C.F.R. § 103.41 (2008) (requiring all classifiable MSBs to be registered with the FDIC, but because virtual currencies exist in a grey area, they do not have to register).

declared as IVTS, it will allow for greater reach from the BSA to close down money laundering loopholes.[117] As part of the redefinition of legal frameworks regarding transactions over the Internet, the new regulations should expand the classifications of MSB to include services that convert between virtual currencies and real world currencies.[118]

As it stands, the five classifications are not enough to categorize websites such as MtGox, but to expand the five classifications to explicitly address services that provide virtual currency transactions would directly incorporate such services under the regulations of the BSA. Once Congress expands existing BSA regulations to cover virtual worlds, prosecutors will have an easier time pressing charges against cyber-money launderers.[119]

B. Extend existing BSA regulations to cover Virtual IVTS.

As soon as Congress updates the BSA to take into account the existence of virtual currencies and services that allow for conversion of virtual currencies into real world

---

[117] *Cf.* Mayer-Schönberger & Crowley, *supra* note 32, at 1825-26 (making the argument for self-regulation on the Internet and that the government should not interfere in regulating activity on the Internet. The authors claim that this is the most effective way for the Internet to police itself, and no amount of government regulation can achieve similar results).

[118] *But see* Nikolei M. Kaplanov, Note, *Nerdy Money: Bitcoin, The Private Digital Currency, And The Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111, 169-171 (arguing against regulation of Bitcoins because prosecutors looking into financial crimes can use the P2P ledgers to investigate sources of irregularities).

[119] *See* Lormel, *supra* note 63 (advocating that MSB definition must be expanded in order for vulnerabilities and workarounds to be closed as the categories are too limited currently, allowing for terrorists and the like to exploit).

money, these services are obligated to be subject to BSA regulations. To that end, these services must implement comprehensive anti-money laundering and financing programs, as stipulated by the BSA.[120] That would ensure that these informal services follow the same rules as that of formal financial institutions. This expansion of regulation into virtual worlds will reduce criminal abuse of these systems and close loopholes.[121]

Under existing regulations, institutions must: identify customers as they open accounts by obtaining information such as the customer's name, address, date of birth, and taxpayer identification number; exercise reasonable efforts to verify the customer's identity; maintain records and information obtained during the identification and verification process; and crosscheck with lists of individuals whose assets have been blocked or frozen.[122] This would mean that websites like MtGox would no longer be able to enjoy the high level of anonymity that it does currently with its user base.[123]

While this does pose some major issues over Internet privacy, that data does not need to be made public, but can be kept as a private record in the event that

---

[120] *See generally* Bank Secrecy Act of 1970, *supra* note 7 (requiring informal value transfer systems to be treated in the same manner as formal institutions).

[121] *See* FINCEN, BANK SECRECY ACT REQUIREMENTS (2007), http://www.fincen.gov/statutes_regs/guidance/pdf/bsa_quickrefguide.pdf, 1 (illustrating that once virtual currencies are deemed MSBs, a transactional trail can be created for all transactions, which will allow the BSA to govern).

[122] *See*, *e.g.*, Money Laundering Prevention, *supra* note 3 (recognizing that these regulations were created for formal financial institutions to ensure that any suspicious CTRs could be traced back to specific transactions and people).

[123] *See*, *e.g.*, Bitcoin Wiki: MtGox, *supra* note 47 (stating that the core premise of Bitcoins and Bitcoin traders such as MtGox revolves around anonymity).

investigations are necessary into specific users. This would be a similar procedure to when individuals open a bank account with any banking institution in the United States. Without this key requirement, it will remain near impossible for law enforcement to track down the identities and sources of those involved in virtual money laundering.[124]

C. Existing regulations must be extended to recognize virtual currencies as legally being the same as real world currencies in order for any policies to be successful

Although to require virtual IVTS to maintain strict identification procedures would appear to be an extreme overreach of regulation, traditional banks implemented similar programs when shifting to online banking in the last ten years.[125] A potential solution for websites and users who want to reduce the amount of personal information needed to register and use the virtual MSB is to create a dual classification account system. What that means is that there will be types of accounts, with differing levels of scrutiny. One type will permit users to engage in financial transactions and the other one will not. The former account

---

[124] *See generally* Press Release, U.S. Dep't of Treasury, Treasury and Federal Financial Regulators Issue Patriot Act Regulations on Customer Identification (Jul. 17, 2002), http://www.treasury.gov/press-center/press-releases/Pages/po3263.aspx (reaffirming that existing identification requirements already exist as part of the PATRIOT act updates to the BSA for formal financial institutions).

[125] *See* FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT (last visited Feb. 10, 2014) http://www.ffiec.gov/pdf/authentication_guidance.pdf (outlining the authentication program that banks within the United States underwent in order to close loopholes in formal financial institutions).

will involve strict adherence to the BSA regulations regarding identification, while the latter account will not.[126]

However, in order to impose any sort of drastic restructuring of the way business is done on the Internet through IVTS will invariably require the support and backing of the FATF.[127] Criminals can easily circumvent any domestic regulations made by the United States to impose changes to the online IVTS system. Consequently, full FATF support is necessary to ensure uniform changes and relative parity of recommendations in how global governments treat the issue of virtual currencies as IVTS.[128]

V. CONCLUSION

As the FBI has acknowledged, the new frontier of money laundering and financial crimes using the new medium of virtual currencies is a brutal reality. With the increasing virtualization of the world and the dramatic growth of virtual economies and currencies in the last decade, law enforcement officers currently lack the ability to prosecute financial criminals hiding in cyberspace due to lagging regulations not suited for the virtual world. Once relegated to the realm of academia, virtual currencies, such as Bitcoin, have become increasingly commonplace as a method of exchange on the Internet. The ability of Internet users to convert virtual currency into real currency

---

[126] *Id.* (analyzing the technology used by the banking industry to authenticate identification).

[127] *See* International Standards, *supra* note 5, at 7 (outlining that the FATF's support is necessarily to ensure global uniformity with regards to new regulations over virtual currencies, as evidenced by the far reaching effects of the FATF recommendations on money laundering).

[128] *See generally* Financial Action Task Force, *supra* note 5 (laying out the functions of the FATF as an inter-governmental body created to make and enforce policies regarding international money laundering).

highlights the integration of the virtual economy into the real world.

In order to rectify that problem, lawmakers must be aware of the challenges faced by law enforcement in tracking down cybercriminals. The legal grey area of virtual worlds poses a specific problem and needs to be rectified in order for successful regulation to occur. As this Comment demonstrates, the use of virtual currencies to conduct illegal financial activities is not only a distinct possibility, but also a likely reality, given the ease with which users can escape regulation and law enforcement. Only when Congress declares virtual worlds and currencies to be IVTS can there be regulations on the vulnerabilities of these platforms. The Department of the Treasury should examine the possibility of classifying virtual worlds and economies as IVTS in order to subject these gaps to the BSA's anti-money laundering regulations. Furthermore, users will have to sacrifice a certain degree of anonymity in order to allow for verification of user identities, similar to that of verification during the banking process.

A major leap from the government is required in order to bridge the gap between the 20th century and 21st century concerning financial crimes. The world will only become increasingly more dependent on the Internet and current regulations are insufficient in dealing with this new challenge. To stand idly by and allow the Internet to remain in a legal grey area concerning financial regulation is not only unreasonable, but also a threat to the foundations of the global economy.